

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059358

(43)Date of publication of application : 25.02.2000

(51)Int.Cl. H04L 9/32
G09C 1/00
H04L 1/16
H04L 29/08

(21)Application number : 10-227410

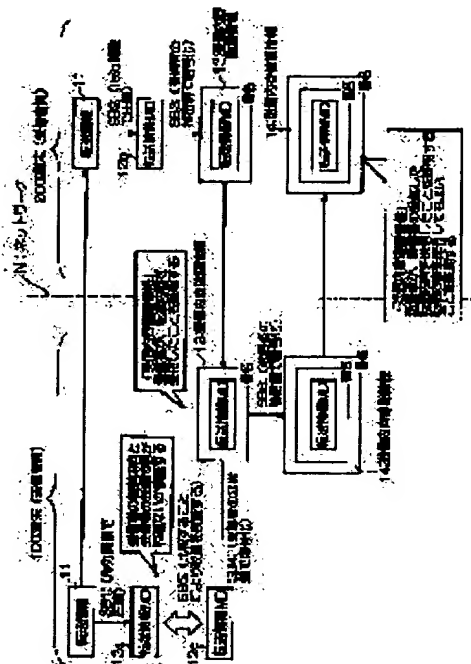
(71)Applicant : MITSUBISHI MATERIALS CORP

(22)Date of filing : 11.08.1998

(72)Inventor : OKUBO TATSUMASA
TOYODA SHOICHI**(54) INFORMATION FALSIFICATION DETECTOR AND COMPUTER READABLE RECORDING MEDIUM STORING FALSIFICATION DETECTION PROGRAM****(57)Abstract:**

PROBLEM TO BE SOLVED: To obtain the information falsification detector that detects falsification of information and a computer readable recording medium that storing a falsification detection program by even in the case of a terminal without a right of decoding received information.

SOLUTION: A system has a terminal 100 and a terminal 200 connecting to the terminal 100 via a network N, and the terminal 100 uses a hash function to compress transfer information 11 and to generate transfer information MD 12a. The terminal 100 transmits the transfer information 11 to the terminal 200 via the network N. After receiving the transfer information 11, the terminal 200 uses a hash function to compress the transfer information 11 and generates transfer information MD12b and encrypts the transfer information MD12b and uses a private key of a recipient to encrypt the transfer information MD12b to generate reception contents confirmation information 13. The terminal 100 compares transfer information MD12c with transfer information MD12b to certify whether or not falsification is made.

**LEGAL STATUS**

[Date of request for examination] 31.03.2000

[Date of sending the examiner's decision of rejection] 26.08.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

BEST AVAILABLE COPY

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号 V

特開2000-59358

(P2000-59358A)

(43)公開日 平成12年2月25日(2000.2.25)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 B 5 K 0 1 3
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 D 5 K 0 1 4
			6 4 0 B 5 K 0 3 4
H 0 4 L 1/16		H 0 4 L 1/16	
29/08		13/00	3 0 7 Z
		審査請求 未請求 請求項の数23 O L (全 15 頁)	

(21)出願番号 特願平10-227410

(22)出願日 平成10年8月11日(1998.8.11)

(71)出願人 000006264

三菱マテリアル株式会社

東京都千代田区大手町1丁目5番1号

(72)発明者 大久保 達真

埼玉県大宮市北袋町1丁目297番地 三菱
マテリアル株式会社総合研究所内

(72)発明者 豊田 祥一

埼玉県大宮市北袋町1丁目297番地 三菱
マテリアル株式会社総合研究所内

(74)代理人 100064908

弁理士 志賀 正武 (外9名)

Fターム(参考) 5K013 AA08 GA03 GA07 GA08 JA00

5K014 AA01 BA00 EA01 HA00

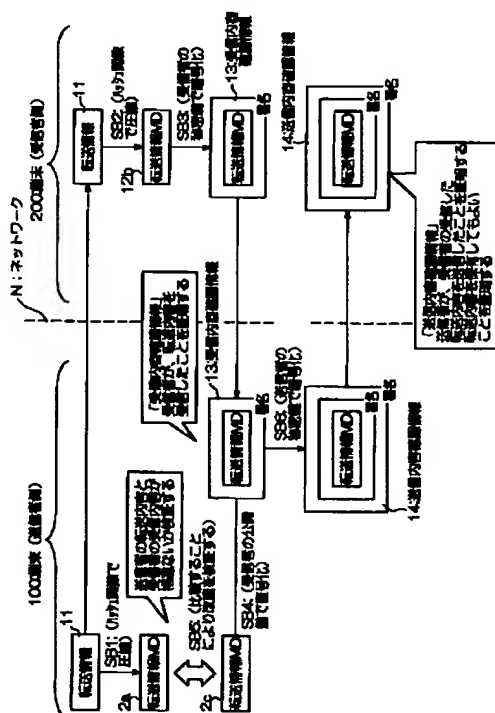
5K034 AA05 DD01 FF01 HH02 HH09

(54)【発明の名称】 情報改竄検知装置および改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】

【課題】 受信した情報を復号化する権利を有しない端末であっても、情報の改竄を検知することができる情報改竄検知装置および改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体を得ること。

【解決手段】 本発明は端末100と端末100にネットワークNを介して接続された端末200とを有しており、端末100は、ハッシュ関数を用いて転送情報11を圧縮して、転送情報MD12aを作成する。端末100は、転送情報11をネットワークNを介して端末200へ送信する。端末200は、転送情報11を受信した後、ハッシュ関数を用いて転送情報11を圧縮して、転送情報MD12bを作成した後、受信者の秘密鍵を利用して転送情報MD12bを暗号化して、受信内容確認情報13を生成する。端末100は、転送情報MD12cと転送情報MD12aとを比較することにより、改竄が行われたか否かを検証する。



【特許請求の範囲】

【請求項 1】 送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、前記ネットワークを介して前記受信内容確認情報を受信する受信手段と、前記送信者側端末から送信される前記情報と前記受信内容確認情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする情報改竄検知装置。

【請求項 2】 前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか 1 つ、または複数組み合わせた情報に基づいて前記受信内容確認情報を作成することを特徴とする請求項 1 に記載の情報改竄検知装置。

【請求項 3】 前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか 1 つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて前記受信内容確認情報を作成することを特徴とする請求項 1 に記載の情報改竄検知装置。

【請求項 4】 前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか 1 つ、または複数組み合わせた情報に対して電子署名したものを前記受信内容確認情報として作成することを特徴とする請求項 1 に記載の情報改竄検知装置。

【請求項 5】 前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか 1 つ、または複数組み合わせた情報を作成し、該組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェスト、および該組み合わせた情報に対して電

子署名をしたものを作成し、

前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか 2 つ以上の情報を組み合わせたものを前記受信内容確認情報として作成することを特徴とする請求項 1 に記載の情報改竄検知装置。

【請求項 6】 送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、

前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、

前記ネットワークを介して前記受信内容確認情報を受信する受信手段と、

前記送信者側端末から送信される前記情報と前記受信内容確認情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段としてコンピュータを機能させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 7】 受信者側に設置された受信者側端末との間でネットワークを介して情報の送受信を行い、送信者側に設置された送信者側端末を有する情報改竄検知装置において、

前記送信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表し、かつ前記受信者側端末により生成された受信内容確認情報を前記ネットワークを介して受信する受信手段と、

前記送信者側端末に設けられ、前記受信手段により受信された前記受信内容確認情報と前記送信者側端末から送信される前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする情報改竄検知装置。

【請求項 8】 前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか 1 つ、または複数組み合わせた情報であることを特徴とする請求項 7 に記載の情報改竄検知装置。

【請求項 9】 前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか 1 つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストであることを特徴とする請求項 7 に記載の情報改竄検知装置。

【請求項 10】 前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか 1 つ、または複数組み合わせた情報に対して電子署名したものであることを特徴とする請求項 7 に記載の情報改竄検知装置。

【請求項 11】 前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか 1 つ、または複数組み合わせた情報に基づいて作成され、該組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェスト、および該組み合わせた情報に対して電子署名をしたものに基づいて作成され、前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか 2 つ以上の情報を組み合わせたものであることを特徴とする請求項 7 に記載の情報改竄検知装置。

【請求項 12】 受信者側に設置された受信者側端末との間でネットワークを介して情報の送受信を行い、送信者側に設置された送信者側端末を有する情報改竄検知装置において、前記送信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表し、かつ前記受信者側端末により生成され、受信内容確認情報を前記ネットワークを介して受信する受信手段と、前記送信者側端末に設けられ、前記受信手段により受信された前記受信内容確認情報と前記送信者側端末から送信される前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段としてコンピュータを機能させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 13】 送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、前記ネットワークを介して前記受信内容確認情報を受信する受信手段と、前記受信内容確認情報に基づいて、送信者側端末が、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を作成し、前記ネットワークを介して前記

受信側端末へ送信する送信内容確認情報作成手段と、前記送信内容確認情報作成手段から送信された前記送信内容確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする情報改竄検知装置。

【請求項 14】 前記送信内容確認情報作成手段は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか 1 つ、または複数組み合わせた情報に基づいて前記送信内容確認情報を作成することを特徴とする請求項 13 に記載の情報改竄検知装置。

【請求項 15】 前記送信内容確認情報作成手段は、前記受信内容確認情報と前記確認情報のうちいずれか 1 つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて前記送信内容確認情報を作成することを特徴とする請求項 13 に記載の情報改竄検知装置。

【請求項 16】 前記送信内容確認情報作成手段は、前記受信内容確認情報と前記確認情報のうちいずれか 1 つ、または複数組み合わせた情報に対して電子署名したものを前記送信内容確認情報として作成することを特徴とする請求項 13 に記載の情報改竄検知装置。

【請求項 17】 前記送信内容確認情報作成手段は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか 1 つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストを前記送信内容確認情報として作成し、

前記受信内容確認情報と前記確認情報のうちいずれか 1 つ、または複数組み合わせた情報に対して電子署名したものを前記送信内容確認情報として作成し、前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか 2 つ以上の情報を組み合わせたものに基づいて前記送信内容確認情報を作成することを特徴とする請求項 13 に記載の情報改竄検知装置。

【請求項 18】 送信者側に設置された送信者側端末との間でネットワークを介して情報の送受信を行い、受信者側に設置された受信者側端末を有する情報改竄検知装置において、

前記受信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、前記受信者側端末に設けられ、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、前記受信者側端末に設けられ、前記受信内容確認情報に基づいて前記送信者側端末により作成される、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を前記ネットワークを介して受信し、該送信内容

確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする情報改竄検知装置。

【請求項 19】 前記送信内容確認情報は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか 1 つ、または複数組み合わせた情報であることを特徴とする請求項 18 に記載の情報改竄検知装置。

【請求項 20】 前記送信内容確認情報は、前記受信内容確認情報と前記確認情報のうちいずれか 1 つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストであることを特徴とする請求項 18 に記載の情報改竄検知装置。

【請求項 21】 前記送信内容確認情報は、前記受信内容確認情報と前記確認情報のうちいずれか 1 つ、または複数組み合わせた情報に対して電子署名したものであることを特徴とする請求項 18 に記載の情報改竄検知装置。

【請求項 22】 前記送信内容確認情報は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか 1 つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて作成され、前記受信内容確認情報と前記確認情報のうちいずれか 1 つ、または複数組み合わせた情報に対して電子署名したものに基いて作成され、前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか 2 つ以上の情報を組み合わせたものであること、を特徴とする請求項 18 に記載の情報改竄検知装置。

【請求項 23】 送信者側に設置された送信者側端末との間でネットワークを介して情報の送受信を行い、受信者側に設置された受信者側端末を有する情報改竄検知装置において、前記受信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、前記受信者側端末に設けられ、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、前記受信者側端末に設けられ、前記受信内容確認情報に基づいて前記送信者側端末により作成される、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を前記ネットワークを介して受信し、該送信内容確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段としてコンピュータを機能させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば、ネットワーク伝送における情報改竄の検知に用いられる情報改竄検知装置および改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【0002】

【従来の技術】従来、情報の改竄を検知する技術（以下、情報改竄検知技術と称する）としては、電子署名技術が情報改竄検知装置により実用化されている。一般的な電子署名技術の例としては、Digital Signature Algorithm や公開鍵暗号方式（例えば RSA 方式）とハッシュ関数（例えば、MD2）と組み合わせるものがある。

【0003】図 7 は、上述した従来の情報改竄検知装置の動作原理を説明する図である。図 7 に示す情報改竄検知装置は、送信者側に設置された送信端末 1 と、該送信端末 1 と図示しないネットワーク（インターネット等）を介して接続され、受信者側に設置された受信端末 6 とから概略構成されている。この情報改竄検知装置において、暗号化、復号化には、公開鍵および秘密鍵が用いられる。この公開鍵と秘密鍵とは、秘密鍵から公開鍵が計算により求めることができる一方、逆に公開鍵から秘密鍵が計算により求めることができないという関係とされている。

【0004】上記構成において、ステップ SA1 では、送信端末 1 は、受信端末 6 へ送信すべき平文 2 を暗号化する。具体的には、送信端末 1 は、受信者（受信端末 6）の公開鍵を利用して平文 2 から暗号文 3 を作成する。次いで、ステップ SA2 では、送信端末 1 は、ハッシュ関数を用いて平文 2 を圧縮して、MD（メッセージダイジェスト）4a を作成する。

【0005】ここで、ハッシュ関数とは、同じ出力値になる任意の 2 つの異なる入力を発見することが計算量的に実行不可能な関数をいい、電子署名等のメカニズムの一部として利用する目的で、長いメッセージから比較的短い一定値長の圧縮データをハッシュ符号として作成するための一方向関数をいう。次に、ステップ SA3 では、送信端末 1 は、送信者（送信端末 1）の秘密鍵を利用して MD 4a から認証子 5 を作成する。この認証子 5 は、暗号文 3 のもとになる平文 2 に対してされた電子署名である。ここでは、電子署名は、メッセージダイジェストの作成という第 1 プロセス、該メッセージダイジェストに対する秘密鍵による暗号化という第 2 プロセスを経てなされるものである。また、電子署名は、上記プロセスの他にメッセージダイジェスト化されていない情報、またはメッセージダイジェストと該情報とを組み合わせたものに対する秘密鍵による暗号化というプロセスを経てなされる場合も含む。

【0006】そして、送信端末 1 は、上記暗号文 3 および認証子 5 をネットワークを介して、受信端末 6 へ送信する。これにより、受信端末 6 は、暗号文 3 および認証

子5を受信した後、まず、ステップSA4で受信者(受信端末6)の秘密鍵を利用して暗号文3を復号化して、平文2を作成する。次いで、ステップSA5では、受信端末6は、ハッシュ関数を用いて復号化された平文2を圧縮することにより、MD4bを作成する。

【0007】また、ステップSA6では、受信端末6は、受信された認証子5を送信者(送信端末1)の公開鍵を利用することにより復号化して、MD4cを作成する。そして、ステップSA7では、受信端末6は、MD4bとMD4cとを比較することにより、転送情報(暗号文3および認証子5)に改竄が行われたか否かの改竄検証を行う。ここで、MD4bとMD4cとが一致している場合には、転送情報に対して改竄が行われていないことを意味する一方、両者が不一致である場合には、転送情報に対して改竄が行われていることを意味する。

【0008】

【発明が解決しようとする課題】ところで、従来の情報改竄検知装置においては、図7に示すように、受信した暗号文3を復号化する権利を有する受信端末6では、転送(送信)途中で転送情報に対して改竄が行われたか否かを、MD4bとMD4cとの比較結果から検知することができる。

【0009】しかしながら、従来の情報改竄検知装置においては、図8に示すように受信した暗号文3を復号化する権利を有しない、言い換えれば、受信者の秘密鍵を有しない受信端末6では、平文2ひいてはMD4bを作成することができないため、転送情報に対する改竄検証を行うことができないという欠点があった。

【0010】したがって、従来の情報改竄検知装置においては、図8に示す受信端末6が更に図示しない別の端末へ転送情報を転送した場合、該端末は、たとえ、暗号文3を復号化する権利を有していても、改竄がいつどこで行われたかを検知することができない。さらに、従来の情報改竄検知装置においては、最初に転送情報を転送する送信端末1がもとの平文2より作成された認証子5(電子署名)でない電子署名を転送した場合であっても、上記端末が改竄を検知することができない。つまり、従来の情報改竄検知装置においては、重要な転送情報に対して改竄が行われた場合、改竄が行われた端末(場所)、時間の特定が重要になるが、これらの検知・特定を行うことができないのである。

【0011】本発明はこのような背景の下になされたもので、受信した情報を復号化する権利を有しない端末であっても、情報の改竄を検知することができる情報改竄検知装置および改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0012】

【課題を解決するための手段】請求項1に記載の発明は、送信者側に設置された送信者側端末と、前記送信者

側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、前記ネットワークを介して前記受信内容確認情報を受信する受信手段と、前記送信者側端末から送信される前記情報と前記受信内容確認情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする。また、請求項2に記載の発明は、請求項1に記載の情報改竄検知装置において、前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか1つ、または複数組み合わせた情報に基づいて前記受信内容確認情報を作成することを特徴とする。また、請求項3に記載の発明は、請求項1に記載の情報改竄検知装置において、前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか1つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて前記受信内容確認情報を作成することを特徴とする。また、請求項4に記載の発明は、請求項1に記載の情報改竄検知装置において、前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか1つ、または複数組み合わせた情報に対して電子署名したものを前記受信内容確認情報として作成することを特徴とする。また、請求項5に記載の発明は、請求項1に記載の情報改竄検知装置において、前記受信内容確認情報作成手段は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか1つ、または複数組み合わせた情報を作成し、該組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェスト、および該組み合わせた情報に対して電子署名をしたものを作成し、前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか2つ以上の情報を組み合わせたものを前記受信内容確認情報として作成することを特徴とする。また、請求項

10

20

30

40

50

50

おいて、前記受信内容確認情報は、前記受信者側端末により受信された前記情報の全部または一部、受信した該情報または一部をハッシュ関数で圧縮したメッセージダイジェスト、送信者に関する送信者情報、受信者に関する受信者情報、通信情報のうち、いずれか1つ、または複数組み合わせた情報に基づいて作成され、該組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェスト、および該組み合わせた情報に対して電子署名をしたものに基づいて作成され、前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか2つ以上の情報を組み合わせたものであることを特徴とする。また、請求項12に記載の発明は、受信者側に設置された受信者側端末との間でネットワークを介して情報の送受信を行い、送信者側に設置された送信者側端末を有する情報改竄検知装置において、前記送信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表し、かつ前記受信者側端末により生成され、受信内容確認情報を前記ネットワークを介して受信する受信手段と、前記送信者側端末に設けられ、前記受信手段により受信された前記受信内容確認情報と前記送信者側端末から送信される前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段としてコンピュータを機能させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体である。また、請求項13に記載の発明は、送信者側に設置された送信者側端末と、前記送信者側端末とネットワークを介して接続され受信者側に設置された受信者側端末とを有し、該送信者側端末と受信者側端末との間で情報の送受信を行い、該情報の改竄を検知する情報改竄検知装置において、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、前記ネットワークを介して前記受信内容確認情報を受信する受信手段と、前記受信内容確認情報に基づいて、送信者側端末が、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を作成し、前記ネットワークを介して前記受信側端末へ送信する送信内容確認情報作成手段と、前記送信内容確認情報作成手段から送信された前記送信内容確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする。また、請求項14に記載の発明は、請求項13に記載の情報改竄検知装置において、前記送信内容確認情報作成手段は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか1つ、または複数組み合わせた情報に基づいて前記送信内容確認情報を作成することを特徴とする。また、請求項15に記載の発明は、請求項13記載の情報改竄検知装置において、前記送信内容確認情報作成手段は、前記

受信内容確認情報と前記確認情報のうちいずれか 1 つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて前記送信内容確認情報を作成することを特徴とする。また、請求項 16 に記載の発明は、請求項 13 に記載の情報改竄検知装置において、前記送信内容確認情報作成手段は、前記受信内容確認情報と前記確認情報のうちいずれか 1 つ、または複数組み合わせた情報に対して電子署名したものを前記送信内容確認情報として作成することを特徴とする。また、請求項 17 に記載の発明は、請求項 13 に記載の情報改竄検知装置において、前記送信内容確認情報作成手段は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか 1 つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストを前記送信内容確認情報として作成し、前記受信内容確認情報と前記確認情報のうちいずれか 1 つ、または複数組み合わせた情報に対して電子署名したものを前記送信内容確認情報として作成し、前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか 2 つ以上の情報を組み合わせたものに基づいて前記送信内容確認情報を作成することを特徴とする。また、請求項 18 に記載の発明は、送信者側に設置された送信者側端末との間でネットワークを介して情報の送受信を行い、受信者側に設置された受信者側端末を有する情報改竄検知装置において、前記受信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、前記受信者側端末に設けられ、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、前記受信者側端末に設けられ、前記受信内容確認情報に基づいて前記送信者側端末により作成される、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を前記ネットワークを介して受信し、該送信内容確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段とを具備することを特徴とする。また、請求項 19 に記載の発明は、請求項 18 に記載の情報改竄検知装置において、前記送信内容確認情報は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか 1 つ、または複数組み合わせた情報であることを特徴とする。また、請求項 20 に記載の発明は、請求項 18 に記載の情報改竄検知装置において、前記送信内容確認情報は、前記受信内容確認情報と前記確認情報のうちいずれか 1 つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストであることを特徴とする。また、請求項 21 に記載の発明は、請求項 18 に記載の情報改竄検知装置において、前記送信内容確認情報は、前記受信内容確認情報と前記確認情報のうちいずれか 1 つ、または複数組み合わせた情報に

対して電子署名したものであることを特徴とする。また、請求項 22 に記載の発明は、請求項 18 に記載の情報改竄検知装置において、前記送信内容確認情報は、前記受信内容確認情報と該受信内容確認情報の内容を確認した旨を表す確認情報のうち、いずれか 1 つ、または複数組み合わせた情報をハッシュ関数で圧縮したメッセージダイジェストに基づいて作成され、前記受信内容確認情報と前記確認情報のうちいずれか 1 つ、または複数組み合わせた情報に対して電子署名したものに基づいて作成され、前記組み合わせた情報、前記メッセージダイジェスト、電子署名したもののうちいずれか 2 つ以上の情報を組み合わせたものであることを特徴とする。また、請求項 23 に記載の発明は、送信者側に設置された送信者側端末との間でネットワークを介して情報の送受信を行い、受信者側に設置された受信者側端末を有する情報改竄検知装置において、前記受信者側端末に設けられ、前記受信者側端末が前記情報を受信したことを確認した旨を表す受信内容確認情報を作成する受信内容確認情報作成手段と、前記受信者側端末に設けられ、前記受信内容確認情報を前記ネットワークを介して送信する送信手段と、前記受信者側端末に設けられ、前記受信内容確認情報に基づいて前記送信者側端末により作成される、前記受信者側端末の受信した情報を送信した旨を表す送信内容確認情報を前記ネットワークを介して受信し、該送信内容確認情報と、前記受信側端末により受信された前記情報とを比較し、この比較結果に基づいて改竄を検知する改竄検知手段としてコンピュータを機能させるための改竄検知プログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0013】

【発明の実施の形態】以下、図面を参照して本発明の実施形態について説明する。図 1 は本発明の一実施形態による情報改竄検知装置の動作原理を説明する図である。この図に示す情報改竄検知装置は、送信者側に設置された端末 100 と、該端末 100 にインターネット等のネットワーク N を介して接続された端末 200 とから概略構成されている。

【0014】上記構成において、ステップ S B 1 では、端末 100 は、ハッシュ関数を用いて転送情報 11 を圧縮して、転送情報 MD (メッセージダイジェスト) 12 a を作成する。この転送情報 MD 12 a は、後述するように送信者の転送内容と受信者の受信内容とが相違していないか否かの検証に用いられる。次いで、端末 100 は、上記転送情報 11 をネットワーク N を介して端末 200 へ送信 (転送) する。

【0015】これにより、端末 200 は、転送情報 11 を受信した後、ステップ S B 2 で、ハッシュ関数を用いて転送情報 11 を圧縮して、転送情報 MD 12 b を作成する。ここで、転送情報 11 に対する改竄が行われていない場合、上記転送情報 MD 12 b と転送情報 MD 12

aとは、同一である。一方、改竄が行われた場合、転送情報MD12bと転送情報MD12aとは、異なる。

【0016】そして、ステップSB3では、端末200は、受信者（端末200）の秘密鍵を利用して転送情報MD12bを暗号化して、受信内容確認情報13を生成する。この受信内容確認情報13は、転送情報MD12bに対して受信者（端末200）による電子署名が行われたものであり、受信者（端末200）が転送内容（転送情報11）を受信したことを証明する情報である。ここでは、電子署名は、メッセージダイジェスト化、暗号化という2つのプロセスを経てなされたものである。また、電子署名は、上記プロセスの他にメッセージダイジェスト化されていない情報、またはメッセージダイジェストと該情報とを組み合わせたものに対する秘密鍵による暗号化というプロセスを経てなされる場合も含む。要は電子署名は、圧縮されている、いないに関わらずある情報に対して秘密鍵により暗号化されたものである。次いで、端末200は、上記受信内容確認情報13をネットワークNを介して端末100へ送信する。

【0017】これにより、端末100は、上記受信内容確認情報13を受信した後、ステップSB4で、受信者（端末200）の公開鍵により受信内容確認情報13を復号化して、転送情報MD12cを作成する。次に、ステップSB5では、端末100は、転送情報MD12cと転送情報MD12aとを比較することにより、改竄が行われたか否かを検証する。具体的には、端末100は、転送情報MD12aと転送情報MD12cとが同一である場合、検証結果を未改竄とする一方、転送情報MD12aと転送情報MD12cとが異なる場合、検証結果を改竄とする。

【0018】次に、ステップSB6では、端末100は、送信者（端末100）の秘密鍵を利用して受信内容確認情報13を暗号化して、送信内容確認情報14を作成する。この送信内容確認情報14は、受信内容確認情報13に対して送信者（端末100）による電子署名が行われたものであり、送信者（端末100）が、受信者（端末200）の受信した転送内容（転送情報11）を送信したことを証明するための情報である。また、送信内容確認情報14は、受信者（端末200）が転送内容（転送情報11）を保有してもよいことを証明するための情報である。

【0019】図2は、本発明の一実施形態による情報改竄検知装置の具体的な構成を示すブロック図である。この図において、図1の各部に対応する部分には同一の符号を付ける。図2に示す端末100において、101は、転送情報11をネットワークNを介して端末200へ送信する情報送信部である。102は、端末200から送信される受信内容確認情報13（図1参照）をネットワークNを介して受信する情報受信部である。

【0020】103は、図1に示すステップSB1、S

B4およびSB5の処理を実行する受信内容確認情報確認部であり、メッセージダイジェスト作成部103a、送信者・通信・受信者情報取得部103bおよび電子署名確認部103cとを有している。受信内容確認情報確認部103において、メッセージダイジェスト作成部103aは、図1に示すステップSB1の処理を実行するものであり、転送情報11をハッシュ関数で圧縮して転送情報MD12aを作成する。送信者・通信・受信者情報取得部103bは、転送情報11、受信内容確認情報13から各送信者情報、通信情報、受信者情報を取得する。

【0021】ここで、送信者情報は、送信者（端末100）に関する情報であり、「送信者名」、「ID」、「公開鍵ID」、「メールアドレス」、信頼性が高い第三者機関によって発行された「電子証明書」等の情報である。また、通信情報は、端末100と端末200との間の通信に関する情報であり、「通信時間」、「受信時間」、「通信方式」、「通信ID」等の情報である。また、受信者情報は、受信者（端末200）に関する情報であり、「受信者名」、「ID」、「公開鍵ID」、「メールアドレス」、信頼性が高い第三者機関によって発行された「電子証明書」等の情報である。図2に示す電子署名確認部103cは、受信内容確認情報13（図1参照）の電子署名が受信者（端末200）によるものであるかを確認する。

【0022】104は、図1に示すステップSB6等の処理を実行する送信内容確認情報作成部であり、メッセージダイジェスト作成部104a、送信者・通信・受信者情報取得部104bおよびメッセージダイジェスト作成部104aとを有している。この送信内容確認情報作成部104は、受信内容確認情報13に基づいて、送信内容確認情報14を作成する。

【0023】この送信内容確認情報作成部104において、メッセージダイジェスト作成部104aは、受信内容確認情報13からメッセージダイジェストを作成する。送信者・通信・受信者情報取得部104bは、上述した送信者・通信・受信者情報取得部103bと同様にして、受信内容確認情報13から送信者情報、通信情報および受信者情報を取得する。電子署名付加部104cは、受信内容確認情報13を送信者（端末100）の秘密鍵により暗号化することにより、受信内容確認情報13に対して（電子）署名を付加する。105は、ネットワークNを介して送信内容確認情報14を端末200へ送信する情報送信部である。

【0024】一方、端末200において、201は、端末100からネットワークNを介して送信される転送情報11を受信する情報受信部である。202は、図1に示すステップSB2およびSB3の処理を実行する受信内容確認情報作成部であり、メッセージダイジェスト作成部202a、送信者・通信・受信者情報取得部202

10

20

30

40

50

bおよび電子署名付加部202cとを有している。この受信内容確認情報作成部202は、転送情報11に基づいて受信内容確認情報13を作成する。

【0025】この受信内容確認情報作成部202において、メッセージダイジェスト作成部202aは、転送情報11をハッシュ関数で圧縮することにより、転送情報MD12b(図1参照)を作成する。送信者・通信・受信者情報取得部202bは、上述した送信者・通信・受信者情報取得部103bと同様にして、転送情報11に関する送信者情報、通信情報および受信者情報を取得する。電子署名付加部202cは、転送情報MD12b

(図1参照)を受信者(端末200)の秘密鍵により暗号化することにより、転送情報MD12bに対して(電子)署名を付加する。ここで、この署名が付加された転送情報MD12bは、受信内容確認情報13である。

【0026】また、205は、端末100から送信された送信内容確認情報14の内容を転送情報11に基づいて確認する送信内容確認情報確認部であり、メッセージダイジェスト作成・取得部205aと、送信者・通信・受信者情報取得部205bと、電子署名確認部205cとを有している。この送信内容確認情報確認部205において、メッセージダイジェスト作成・取得部205aは、上述したメッセージダイジェストを作成する機能と、受信内容確認情報作成部202のメッセージダイジェスト作成部202aによりすでに作成された転送情報MD12b(図1参照)を取得する機能とを有する。ここで、上記転送情報MD12bを取得した場合には、メッセージダイジェスト作成・取得部205aは、メッセージダイジェストを作成しない。送信者・通信・受信者情報取得部205bは、上述した送信者・通信・受信者情報取得部103bと同様にして、送信者情報、通信情報および受信者情報を取得する。電子署名確認部205cは、送信者(端末100)の公開鍵を用いて、受信内容確認情報13に対する署名を確認する。

【0027】次に、上述した一実施形態による情報改竄検知装置の動作について図3～図6に示すフローチャートを参照しつつ説明する。図3は、図2に示す受信内容確認情報確認部103の動作を説明するフローチャートであり、図4は、図2に示す送信内容確認情報作成部104の動作を説明するフローチャートである。また、図5は、図2に示す受信内容確認情報作成部202の動作を説明するフローチャートであり、図6は、図2に示す送信内容確認情報確認部205の動作を説明するフローチャートである。

【0028】図2において、端末100における転送情報11が情報送信部101によりネットワークNを介して端末200へ送信されると、該転送情報11は、端末200の情報受信部201により受信される。これにより、端末200の受信内容確認情報作成部202は、図5に示すフローチャートに従って受信内容確認情報13

を生成する。

【0029】具体的には、図5に示すステップSE1では、受信内容確認情報作成部202は、受信内容(転送情報11)を入力する。これにより、ステップSE2では、メッセージダイジェスト作成部202aは、受信内容(転送情報11)をハッシュ関数で圧縮してメッセージダイジェスト(図1:転送情報MD12b)を作成する。なお、図5に示す例では、ステップSE2の処理を実行することなく、ステップSE1からステップSE6へ進んでもよい。

【0030】また、ステップSE3～SE5では、受信内容確認情報作成部202は、送信者情報(送信者名、ID、公開鍵ID、メールアドレス、電子証明書等)、受信者情報(受信者名、ID、公開鍵ID、メールアドレス、電子証明書等)、通信情報(送信時間、受信時間、通信方式、通信ID等)を転送情報11から取り込む。

【0031】これにより、ステップSE6では、送信者・通信・受信者情報取得部202bは、ステップSE3～SE5で入力された送信者情報、受信者情報および通信情報を取得した受信内容確認情報作成部202は、上述した受信内容(転送情報11)と、転送情報MD12b、送信者情報、受信者情報、通信情報等の各情報とを統合する。ここで、情報の統合とは、ハッシュ関数で圧縮された転送情報MD12bの全部または一部と、送信者情報における送信者名、ID等、受信者情報における受信者名、ID等、通信情報における送信時間、受信時間等のうち1つまたは複数の情報とを組み合わせることをいう。

【0032】次に、ステップSE7では、メッセージダイジェスト作成部202aは、ステップSE6で統合された情報をハッシュ関数で圧縮することにより、メッセージダイジェストを作成する。次いで、ステップSE8では、電子署名付加部202cは、ステップSE7で作成されたメッセージダイジェストを受信者の秘密鍵で暗号化することにより、メッセージダイジェストに対して、電子署名を付加する。そして、ステップSE9では、受信内容確認情報作成部202は、各情報を統合化することにより、図1に示す受信内容確認情報13を作成した後、これを情報送信部203へ出力する。また、メッセージダイジェスト作成部202aは、必要に応じて転送情報MD12bを送信内容確認情報確認部205のメッセージダイジェスト作成・取得部205aへ出力する。この場合、メッセージダイジェスト作成・取得部205aは、メッセージダイジェストの作成を行うことなく、上記転送情報MD12bを取得する。

【0033】そして、上記受信内容確認情報13は、情報送信部203によりネットワークNを介して端末100へ送信された後、端末100の情報受信部102により受信される。これにより、端末100の受信内容確認

10

20

30

40

50

情報確認部 103 は、図 3 に示すフローチャートに従って、受信内容確認情報 13 の内容を確認することにより、改竄を検知する。

【0034】具体的には、図 3 に示すステップ SC1 では、受信内容確認情報確認部 103 は、情報受信部 102 により受信された受信内容確認情報 13 を入力した後、ステップ SC2 へ進む。ステップ SC2 では、メッセージダイジェスト作成部 103a は、受信者の公開鍵を用いて受信内容確認情報 13 を復号化することにより、メッセージダイジェスト（図 1：転送情報 MD12c）を作成（取得）する。

【0035】そして、ステップ SC3 では、電子署名確認部 103c は、受信者（端末 200）の公開鍵を用いて、受信内容確認情報 13 が受信者により署名されたものであるか否かを確認する。ここで、受信内容確認情報 13 が受信者（端末 200）の公開鍵で復号化できた場合、受信内容確認情報 13 は、受信者により署名されたものであり、一方、受信内容確認情報 13 が受信者の公開鍵で復号化できなかった場合、受信内容確認情報 13 は受信者により署名されなかったものである。

【0036】次に、ステップ SC4 では、受信内容確認情報確認部 103 は、ステップ SC3 の確認結果から、受信内容確認情報 13 の署名が受信者（端末 200）の署名であるか否かを判断し、同判断結果が「NO」の場合、改竄もしくは通信エラーが発生したものとす。一方、ステップ SC4 の判断結果が「YES」の場合、受信内容確認情報確認部 103 は、ステップ SC5 へ進む。

【0037】ステップ SC5 では、受信内容確認情報 13 に含まれている各種情報を分類する。ここで、上記各種情報としては、受信情報内容、前述した送信者情報、受信者情報、通信情報、メッセージダイジェスト（転送情報 MD12c）等がある。

【0038】また、受信内容確認情報確認部 103 は、ステップ SC6 へ進み、転送情報 11、送信者が転送した、通信に関する送信者情報、通信情報、受信者情報等を入力する。次に、ステップ SC7 では、受信内容確認情報確認部 103 のメッセージダイジェスト作成部 103a は、転送情報 11 をハッシュ関数で圧縮して転送情報 MD12a（図 1 参照）を作成する。

【0039】そして、受信内容確認情報確認部 103 は、ステップ SC9～SC12 で受信内容と送信内容とを比較することにより、受信内容の検証を情報毎に行う。そして、ステップ SC13 では、受信内容確認情報確認部 103 は、上記ステップ SC9～SC12 の検証結果を受けて、受信内容が送信内容と相違ないか否かを判断し、同判断結果が「NO」の場合、改竄もしくは通信エラーが発生しているものとする。一方、受信内容確認情報確認部 103 は、受信内容が送信内容と相違していない場合、SC13 の判断結果を「YES」として、

改竄が発生していないものとする。

【0040】次いで、送信内容確認情報作成部 104 は、図 4 に示すフローチャートに従って、送信内容確認情報 14（図 1 参照）を作成する処理を実行する。すなわち、送信内容確認情報作成部 104 は、図 4 に示すステップ SD1 で受信内容確認情報 13 を入力した後、ステップ SD2 で受信内容確認情報承認情報を生成する。ここで、受信内容確認情報承認情報とは、受信内容確認情報確認部 103 が受信内容確認情報 13 の内容を承認（確認）した旨を示す情報である。この承認（確認）した旨を示す情報は、承認した時間、端末、承認者（一実施形態では送信者）に関する情報を元に生成される。

【0041】次いで、ステップ SD3 では、送信内容確認情報作成部 104 は、受信内容確認情報 13 と受信内容確認情報承認情報とを統合する。次に、ステップ SD4 では、メッセージダイジェスト作成部 104a は、ステップ SD3 において統合された情報のメッセージダイジェストを取得した後、ステップ SD5 へ進む。ステップ SD5 では、電子署名付加部 104c は、送信者（端末 100）の秘密鍵により暗号化することにより、メッセージダイジェストに対して署名を行う。

【0042】そして、ステップ SD6 では、送信内容確認情報作成部 104 は、ステップ SD3 における各種情報とステップ SD5 において署名されたメッセージダイジェストとを統合化する。これにより、送信内容確認情報作成部 104 においては、送信内容確認情報 14 が作成され、該送信内容確認情報 14 は、情報送信部 105 へ出力される。

【0043】そして、上記送信内容確認情報 14 は、情報送信部 105 により、ネットワーク N を介して端末 200 へ送信された後、端末 200 の情報受信部 204 により受信される。

【0044】これにより、端末 200 の送信内容確認情報確認部 205 は、図 6 に示すフローチャートに従って、送信内容確認情報 14 の確認を実行する。具体的には、図 6 に示すステップ SF1 では、送信内容確認情報確認部 205 は、情報受信部 204 により受信された送信内容確認情報 14 を入力した後、ステップ SF2 へ進む。ステップ SF2 では、メッセージダイジェスト作成・取得部 205a は、送信者（端末 100）の公開鍵を用いて送信内容確認情報 14 を復号化することにより、メッセージダイジェストを作成（取得）する。

【0045】そして、ステップ SF3 では、電子署名確認部 205c は、送信者（端末 100）の公開鍵を用いて、送信内容確認情報 14 が送信者により署名されたものであるか否かを確認する。ここで、送信内容確認情報 14 が送信者（端末 100）の公開鍵で復号化できた場合、送信内容確認情報 14 は、送信者により署名されたものであり、一方、送信内容確認情報 14 が送信者の公開鍵で復号化できなかった場合、送信内容確認情報 14

は送信者により署名されなかったものである。

【0046】次に、ステップSF4では、送信内容確認情報確認部205は、ステップSF3の確認結果から、送信内容確認情報14の署名が送信者（端末100）の署名であるか否かを判断し、同判断結果が「NO」の場合、改竄もしくは通信エラーが発生したものとす。一方、ステップSF4の判断結果が「YES」の場合、送信内容確認情報確認部205は、ステップSF5へ進む。

【0047】ステップSF5では、送信内容確認情報14に含まれている各種情報を分類する。ここで、上記各種情報としては、受信情報内容、前述した送信者情報、受信者情報、通信情報、メッセージダイジェスト等がある。

【0048】また、送信内容確認情報確認部205は、ステップSF6へ進み、受信した転送情報11、送信者が転送した、通信に関する送信者情報、通信情報、受信者情報等を入力する。次に、ステップSF7では、送信内容確認情報確認部205のメッセージダイジェスト作成・取得部205aは、転送情報11をハッシュ関数で圧縮して転送情報MD12b（メッセージダイジェスト）を作成する。ただし、メッセージダイジェスト作成・取得部205aは、メッセージダイジェスト作成部202aから転送情報MD12bを取得した場合、上記作成動作を行わない。

【0049】そして、送信内容確認情報確認部205は、ステップSF9～SF12で受信内容と送信内容とを比較することにより、受信内容の検証を情報毎に行う。そして、ステップSF13では、送信内容確認情報確認部205は、上記ステップSF9～SF12の検証結果を受けて、受信内容が送信内容と相違ないか否かを判断し、同判断結果が「NO」の場合、改竄もしくは通信エラーが発生しているものとする。一方、送信内容確認情報確認部205は、受信内容が送信内容と相違していない場合、SF13の判断結果を「YES」として、改竄が発生していないものとする。

【0050】以上説明したように、上述した一実施形態による情報改竄検知装置によれば、受信内容確認情報13、送信内容確認情報14を用いて改竄検知を行うように構成したので、受信した情報を復号化する権利を有しない端末であっても、情報の改竄を検知することができる。

【0051】以上本発明の実施形態について詳述してきたが、具体的な構成はこの実施形態に限定されるものではなく本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。例えば、上述した一実施形態による情報改竄検知装置においては、上述した機能を実現するための改竄検知プログラムを、フレキシブルディスク、CD-ROM、光磁気ディスク、ICカード、DVD-ROM等のコンピュータ読み取り可能な記録媒体

に記録して、この記録媒体に記録された改竄検知プログラムをコンピュータシステムに読み込ませて実行させることにより、情報の改竄検知をおこなってもよい。

【0052】また、上記改竄検知プログラムは、フロッピーディスク、CD-ROM等の可搬媒体や、ハードディスク等の記憶装置等に、その全体あるいは一部が記録され、あるいは記憶されている。その改竄検知プログラムは、コンピュータにより読みとられて、動作の全部あるいは一部が実行される。また、ここでいう記録媒体は、光磁気ディスク等のように改竄検知プログラムを静的に記録しているものに限らず、インターネットの専用線、電話回線等の通信回線を通して改竄検知プログラムを送信する場合の通信回線のように、短時間の間、動的に改竄検知プログラムを保持しているもの、その場合のサーバやコンピュータ内部のメモリのように、一定時間改竄検知プログラムを保持しているものも含むものとする。

【0053】

【発明の効果】以上説明したように、本発明によれば、受信内容確認情報、送信内容確認情報を用いて改竄検知を行うように構成したので、受信した情報を復号化する権利を有しない端末であっても、情報の改竄を検知することができる。

【図面の簡単な説明】

【図1】 本発明の一実施形態による情報改竄検知装置の動作原理を説明するブロック図である。

【図2】 同一実施形態による情報改竄検知装置の構成を示すブロック図である。

【図3】 図2に示す受信内容確認情報確認部103の動作を説明するフローチャートである。

【図4】 図2に示す送信内容確認情報作成部104の動作を説明するフローチャートである。

【図5】 図2に示す受信内容確認情報作成部202の動作を説明するフローチャートである。

【図6】 図2に示す送信内容確認情報確認部205の動作を説明するフローチャートである。

【図7】 従来の情報改竄検知装置の動作原理を説明する図である。

【図8】 従来の情報改竄検知装置の欠点を説明する図である。

【符号の説明】

100 端末

101 情報送信部

102 情報受信部

103 受信内容確認情報確認部

103a メッセージダイジェスト作成部

103b 送信者・通信・受信者情報取得部

103c 電子署名確認部

104 送信内容確認情報作成部

104a メッセージダイジェスト作成部

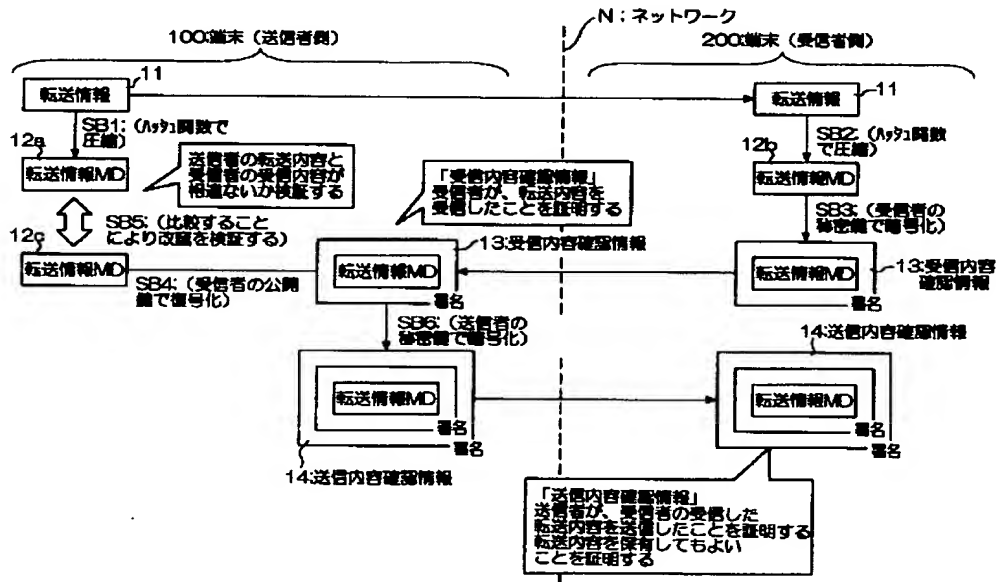
21

22

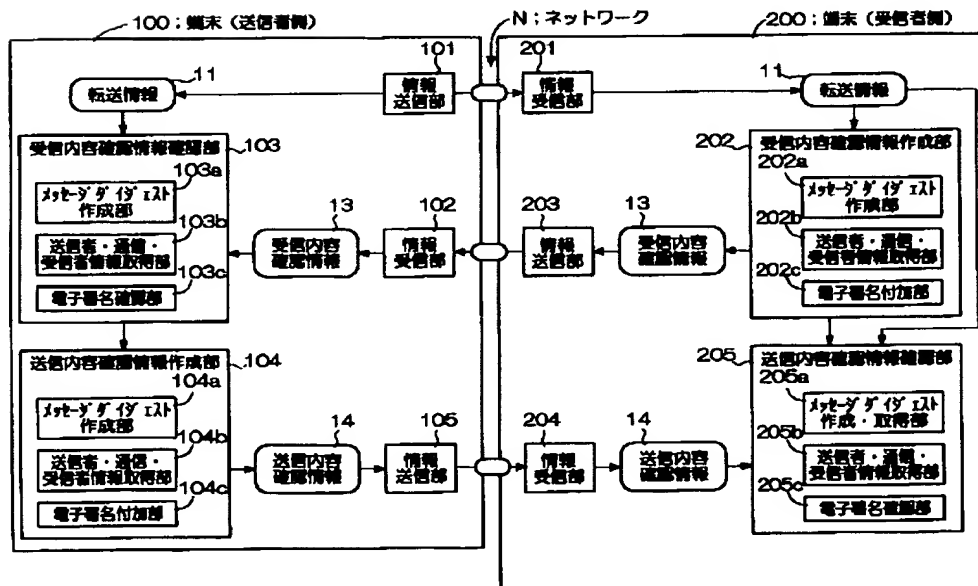
104b 送信者・通信・受信者情報取得部
 104c 電子署名付加部
 105 情報送信部
 200 端末
 201 情報受信部
 202 受信内容確認情報作成部
 202a メッセージダイジェスト作成部
 202b 送信者・通信・受信者情報取得部

202c 電子署名付加部
 203 情報送信部
 204 情報受信部
 205 送信内容確認情報確認部
 205a メッセージダイジェスト作成・取得部
 205b 送信者・通信・受信者情報取得部
 205c 電子署名確認部

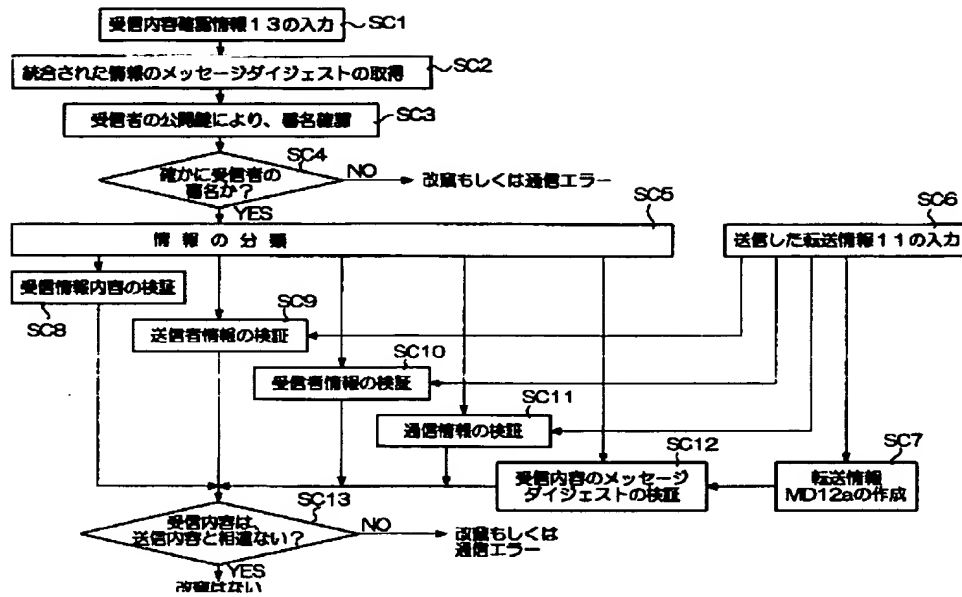
【図1】



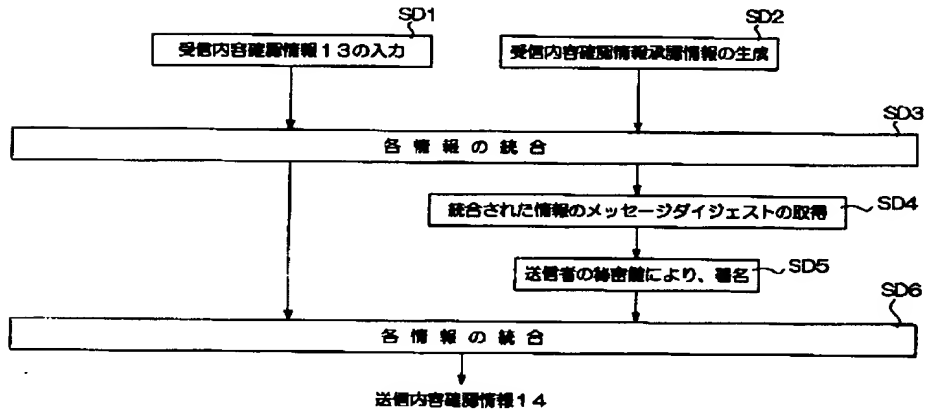
【図2】



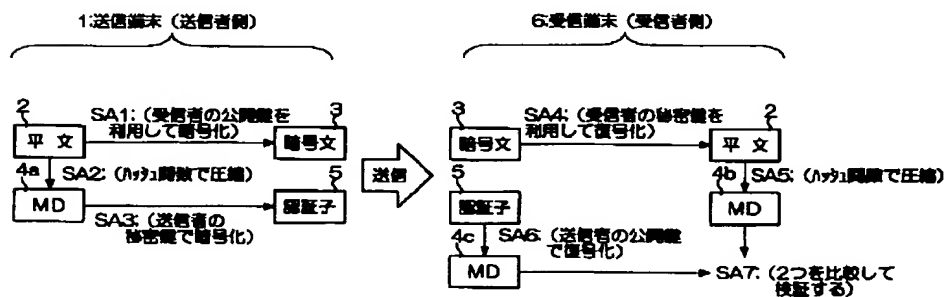
【図 3】



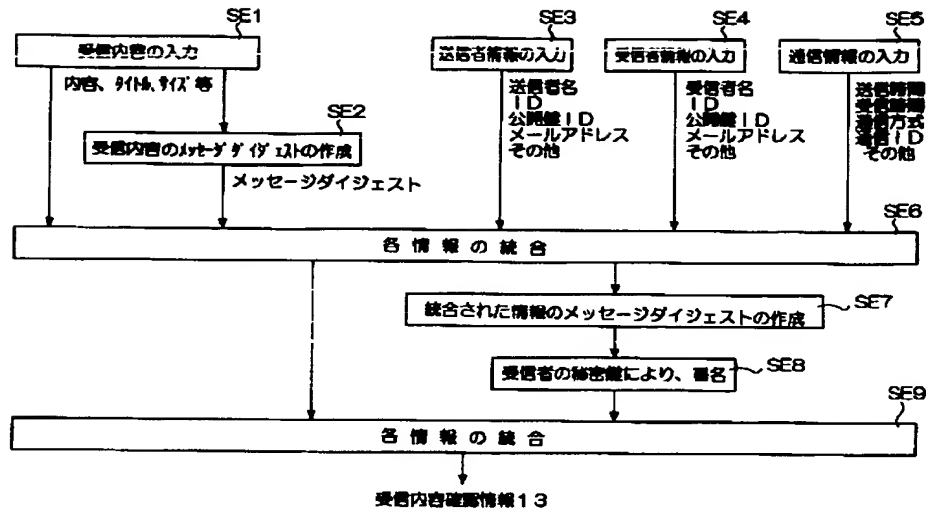
【図 4】



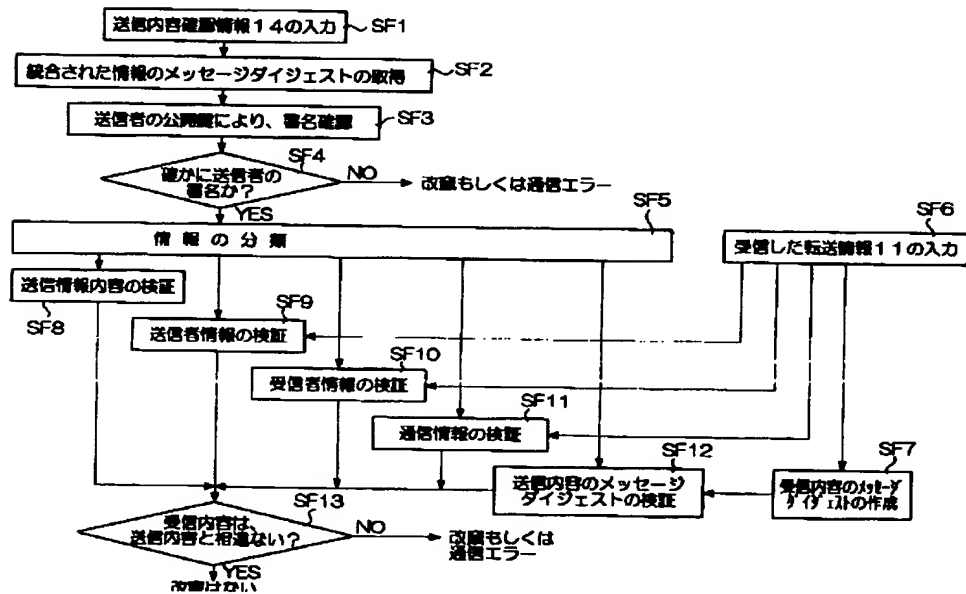
【図 7】



【図 5】



【図 6】



【図 8】

